

**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF DELAWARE**

ROTHSCHILD BROADCAST DISTRIBUTION SYSTEMS, LLC	§	
	§	
	§	
Plaintiff,	§	Case No:
	§	
vs.	§	PATENT CASE
	§	
FRONTPONT SECURITY SOLUTIONS, LLC,	§	
	§	
	§	
Defendant.	§	
	§	
	§	

---

**COMPLAINT**

Plaintiff Rothschild Broadcast Distribution Systems, LLC (“Plaintiff” or “RBDS”) files this Complaint against Frontpoint Security Solutions, LLC (“Defendant” or “Frontpoint”) for infringement of United States Patent No. 8,856,221 (hereinafter “the ‘221 Patent”).

**PARTIES AND JURISDICTION**

1. This is an action for patent infringement under Title 35 of the United States Code. Plaintiff is seeking injunctive relief as well as damages.

2. Jurisdiction is proper in this Court pursuant to 28 U.S.C. §§ 1331 (Federal Question) and 1338(a) (Patents) because this is a civil action for patent infringement arising under the United States patent statutes.

3. Plaintiff is a Texas limited liability company with an office at 1400 Preston Road, Suite 400, Plano, Texas 75093.

4. On information and belief, Defendant is a Delaware corporation, with its principal place of business at 1595 Spring Hill Road, Suite 110, Vienna, Virginia 22182.

5. On information and belief, this Court has personal jurisdiction over Defendant

because Defendant has committed, and continues to commit, acts of infringement in this District, has conducted business in this District, and/or has engaged in continuous and systematic activities in this District.

6. On information and belief, Defendant's instrumentalities that are alleged herein to infringe were and continue to be used, imported, offered for sale, and/or sold in this District.

**VENUE**

7. Venue is proper in this District pursuant to 28 U.S.C. § 1400(b) because Defendant is deemed to reside in this District as it is a Delaware limited liability company.

**COUNT I**  
**(INFRINGEMENT OF UNITED STATES PATENT NO 8,856,221)**

8. Plaintiff incorporates paragraphs 1-7 herein by reference.

9. This cause of action arises under the patent laws of the United States and, in particular, under 35 U.S.C. §§ 271, et seq.

10. Plaintiff is the owner by assignment of the '221 Patent with sole rights to enforce the '221 Patent and sue infringers.

11. A copy of the '221 Patent, titled "System and Method for Storing Broadcast Content in a Cloud-based Computing Environment," is attached hereto as Exhibit A.

12. The '221 Patent is valid, enforceable, and was duly issued in full compliance with Title 35 of the United States Code.

13. Upon information and belief, Defendant has infringed and continues to infringe one or more claims, including at least Claim 1, of the '221 Patent by making, using, importing, selling, and/or offering for media content storage and delivery systems and services covered by one or more claims of the '221 Patent.

14. Defendant sells, offers to sell, and/or uses media content storage and delivery

systems and services, including, without limitation, the Frontpoint Security Home Monitoring system, and any similar products (“Product”), which infringes at least Claim 1 of the ‘221 Patent.

15. The Product necessarily includes at least one server for hosting and storing media content for customers. For example, the Product necessarily includes at least one server to store recorded security videos.

16. The at least one server necessarily includes a first receiver configured to receive a request message including data indicating requested media content (e.g., the server must have infrastructure to receive a request to store recorded security videos or to stream recorded video on a smartphone; additionally, the request message must contain data that identifies the video to be stored or streamed) and a consumer device identifier corresponding to a consumer device (e.g., the user credentials are used to tie a smartphone and user account to particular cameras and the videos they produce).

17. The Product necessarily includes a processor to determine whether the consumer device identifier corresponds to the registered consumer device (e.g., the server must authenticate a user’s credentials to ensure that the credentials match those registered with a security camera which the user would like to access).

18. The Product provides for both media downloads and/or storage, and media streaming. A processor within the Product necessarily determines whether the request received from a customer is a request for storage (e.g., recording or storing content) or content (e.g., streaming of media content).

19. The server verifies that media content identified in the media data of the storage request message (e.g., request to record content) is available for storage in order to prevent data

errors that would result from attempting to store content that is not available for storage. The server must verify that the media content (e.g. specific recording from a specific camera) identified in the media data of the storage request message is available for storage in order to prevent data errors that would result from attempting to store content that is not available for storage (e.g. the server must verify that a particular security camera is adequately connected to the internet as to allow for video recording and storage on the cloud; additionally, a user's ability to store video is limited to a certain amount of memory usage based upon their subscription, thus media content may not be available for storage if a user is already above their memory limit).

20. If a customer requests content (e.g., live streaming of media content), then a processor within the Product necessarily initiates delivery of the content to the customer's device. The server will initiate delivery of the requested media content to the consumer device (e.g. stream live camera feed to a smartphone or tablet) if the request message is a content request message (e.g. request for live streaming).

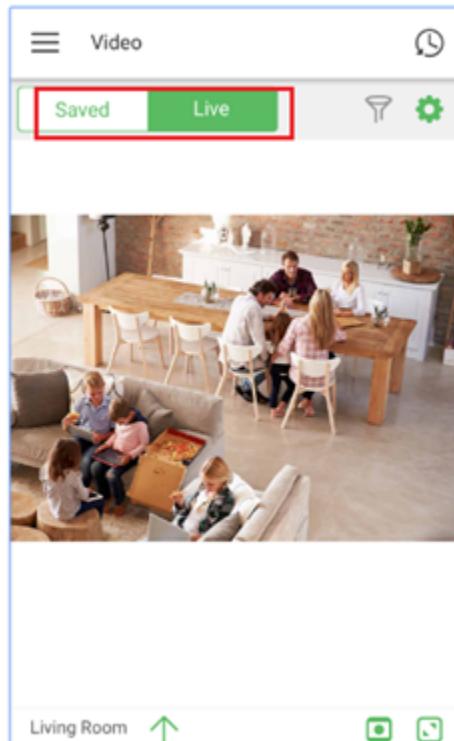
21. The media data includes time data that indicates a length of time to store the requested media content (e.g. a user is allowed to store videos for maximum of 30 days as based upon their subscription level).

22. The server must first determine whether the requested media content exists prior to initiating delivery in order to prevent data errors that would result from attempting to transmit media content that does not exist (e.g. the server must verify that a particular security camera is adequately connected to the internet as to allow for video recording and streaming).

23. After the processor determines whether the requested media content is available, it determines whether there are restrictions associated with the requested media

content (e.g., subscription level, component protocols, etc.).

24. The various elements of Claim 1 are further illustrated in the various publicly available screen shots provided below:



<https://play.google.com/store/apps/details?id=com.alarm.alarmmobile.android.frontpoint&hl=en>

#### How much cloud storage does Frontpoint offer?

Frontpoint's camera plan offers 1,000 clips a month of free storage. This number is regardless of the clip length, and it will reset every month. Also, any clips triggered by alarm events will not count against your clip limit. If you go over 1,000 clips in a month, the system will kick out the oldest clip to make room for the newest, unless you mark a clip to be saved. Lastly, you can choose to save any of the clips locally to your computer. And you have the option to delete clips from the cloud at any time.

#### How long are the recorded clips?

System triggered and alarm triggered clips can be 50-60 seconds long. In the event of an alarm, you can tell the system to record 15 back-to-back clips essentially making the camera record for 15 minutes. Motion triggered clips can be 10-40 seconds per clip.

<http://asecurecam.com/frontpoint-security-camera-review/>

	Interactive Plan	Ultimate Plan
Monthly Price	\$44.99	\$49.99
Cellular Alarm Monitoring	YES	YES
Internet Required	NO	Cameras Require Internet Bandwidth Optimized
24/7 Intrusion & Fire Protection	YES	YES
UL-Listed Monitoring	YES	YES
Environmental Protection	YES	YES
Life Safety	YES	YES
Crash & Smash Protection	YES	YES
<a href="http://asecurecam.com/frontpoint-security-camera-review/">http://asecurecam.com/frontpoint-security-camera-review/</a>		
Email & Text Alerts	YES	YES
Remote Access & Control	YES	YES
Light Automation	YES	YES
GEO Location Services	YES	YES
Automated Door Locks	NO	YES
Energy Management Control	NO	YES
Image Sensor	YES	YES
Live Video Streaming	NO	YES
HD & Night Vision Capabilities	NO	YES
<a href="http://asecurecam.com/frontpoint-security-camera-review/">http://asecurecam.com/frontpoint-security-camera-review/</a>		

Motion Activated Video Recording	NO	YES
Clip Storage, up to 50MB	NO	YES

<http://asecurecam.com/frontpoint-security-camera-review/>

The accused product utilizes a first server (e.g. a cloud server used to store recorded security videos).

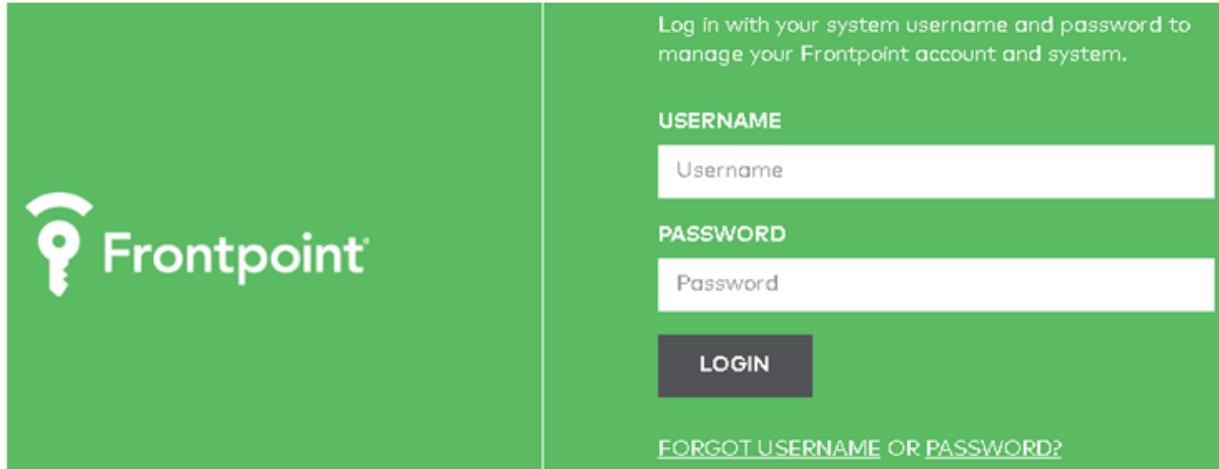
**How much cloud storage does Frontpoint offer?**

Frontpoint's camera plan offers 1,000 clips a month of free storage. This number is regardless of the clip length, and it will reset every month. Also, any clips triggered by alarm events will not count against your clip limit. If you go over 1,000 clips in a month, the system will kick out the oldest clip to make room for the newest, unless you mark a clip to be saved. Lastly, you can choose to save any of the clips locally to your computer. And you have the option to delete clips from the cloud at any time.

**How long are the recorded clips?**

System triggered and alarm triggered clips can be 50-60 seconds long. In the event of an alarm, you can tell the system to record 15 back-to-back clips essentially making the camera record for 15 minutes. Motion triggered clips can be 10-40 seconds per clip.

<http://asecurecam.com/frontpoint-security-camera-review/>



The image shows the Frontpoint login page. On the left, there is a large green background with the Frontpoint logo, which consists of a stylized key icon and the word "Frontpoint". On the right, there is a white login form. At the top of the form, it says "Log in with your system username and password to manage your Frontpoint account and system." Below this, there are two input fields: "USERNAME" and "PASSWORD", each with a corresponding text input box. Below the password input box is a "LOGIN" button. At the bottom of the form, there is a link "FORGOT USERNAME OR PASSWORD?".

<https://my.frontpointsecurity.com/login>

25 Defendant's actions complained of herein will continue unless Defendant is enjoined by this court.

26. Defendant's actions complained of herein is causing irreparable harm and monetary damage to Plaintiff and will continue to do so unless and until Defendant is enjoined and restrained by this Court.

27. Plaintiff is in compliance with 35 U.S.C. § 287.

**PRAYER FOR RELIEF**

WHEREFORE, Plaintiff asks the Court to:

- (a) Enter judgment for Plaintiff on this Complaint on all causes of action asserted herein;
- (b) Enter an Order enjoining Defendant, its agents, officers, servants, employees, attorneys, and all persons in active concert or participation with Defendant who receives notice of the order from further infringement of United States Patent No. 8,856,221 (or, in the alternative, awarding Plaintiff a running royalty from the time of judgment going forward);
- (c) Award Plaintiff damages resulting from Defendant's infringement in accordance with 35 U.S.C. § 284;
- (d) Award Plaintiff pre-judgment and post-judgment interest and costs; and
- (e) Award Plaintiff such further relief to which the Court finds Plaintiff entitled under law or equity.

Dated: January 31, 2018

Respectfully submitted,

*/s/ Stamatis Stamoulis*  
**STAMATIOS STAMOULIS (#4606)**  
**STAMOULIS & WEINBLATT LLC**  
Two Fox Point Centre  
6 Denny Rd.  
Suite 307  
Wilmington, DE 19809  
(302) 999-1540  
stamoulis@swdelaw.com

**ATTORNEYS FOR PLAINTIFF**